Here are several recent HIPAA e-news items.
Ken

[hipaalive] Re: GENERAL: HIPAA Implementaion Plan
[hipaalive] RE: Dental Insurance information.
[hipaalive] RE: GENERAL: Audit Trail Storage Requirements
[hipaalive] RE: [hipaalive]More AHA - cost savings
[hipaalive] RE: GENERAL: Audit Trail

********** [hipaalive] Re: GENERAL: HIPAA Implementaion Plan **********
>>> matperry@nortelnetworks.com 02/06/01 06:39AM >>>

I think you would be well served if you divided your implementation plan for HIPAA into 2 main categories; Privacy and Security.

The final Privacy Rules have been released about 6 weeks ago and can be found on the Department of Health and Human Services (DHHS) web site. The final rules for Security have yet to be released, but the Proposed Rules are also posted on the DHHS site and will give you a good head start there.

I too am responsible for devising an implementation plan for HIPAA, only for the Security Rules however. So I can offer you my approach in that and hopefully it help you out.

DHHS utilized extensive research into current marketplace security standards to develop the security standards in the proposed regulations. The security standards would not require the use of specific technologies or particular hardware or software, but instead would require Health Plans, Health Care Clearinghouses and Health Care Providers, who electronically store and transmit Health Information, to comply with certain minimum threshold protocols and procedures in four broad categories. These categories relate to different aspects of ensuring the integrity, confidentiality and availability of electronically stored and transmitted Health Information, as follows: (i) administrative procedures (ii) physical safeguards, (iii) technical protections relating top data storage and (iv) technical protections relating to access to and transmission of data.

1) Administrative Roles and Responsibilities: These are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.
Examples:
Contingency Plan for Data Backup, Data Recovery, Emergency Mode Operation
Information Access Control: Access Authorization, Establishment, and Modification
Personnel Security: Clearance Procedures, All system users (to include maintenance) are trained in security
Security Incident Procedures: both reporting and response
Security Management: Risk analysis and management - sanction and security policies
Termination Procedures: Combos and locks changed, all access cards are returned
Training: General Security Awareness, virus protection, incident reporting, etc....

2) Physical Safeguards: Protecting data integrity, confidentiality,and availability in relation to the protection of computer systems and facilities from natural disasters, intrusions, and the sort.
Examples:
Media Controls: Access Control, Accountability, Data Backup, Data Storage, Disposal
Physical Access Controls: Disaster Recovery, Facility Security Plan, Maintenance Records, Sign-in for visitors, etc...
Secure Workstation Location:pretty self explanatory

3) Technical Security Services: Processes put in lace to protect, control, and monitor information access

Examples:
Access Control: This is the method of restricting access to resources and allowing privileged entities access. (Role based access, user based access, Discretionary Access Control, Mandatory Access Control, etc...)
Audit Controls: You will want mechanisms in place to record and examine system activity
Entity Authentication: Automatic log off, Tokens, PINs, Passwords, Biometrics, etc...
Cryptography: Encryption, Digital Signatures, Key Management

4) Technical Security Mechanisms: To guard against unauthorized access to data that is transmitted over a communications network
Examples:
Network Controls: Audit Trails, Event Reporting, Integrity Controls, Encryption, etc....

5) Electronic Signatures: Methods used so that the identity of signer and the integrity of the data can be verified. (Not mandatory according to the Proposed Rules, but if used, must follow guidelines)
Examples: Message integrity, Multiple Signatures, Non-Repudiation, Transportability, User authentication, etc...

That is the method I used in developing the Security portion of HIPAA. Obviously in there somewhere should be network assessments and audits to

make sure you identify glaring weaknesses or vulnerabilities in your network. Also, there is more added to each category mentioned above and all must be implemented and followed for compliance. I hope this gives you a kick start atleast in the security portion of it.

Matthew Perry
GPS Security Solutions; Nortel Networks
matperry@nortelnetworks.com

********** [hipaalive] RE: Dental Insurance information. **********
>>> tom.hanks@beaconpartners.com 02/03/01 09:21AM >>>

1) Under HIPAA protected health information (PHI) includes all individually identifiable health information and even includes pure demographics that are not related to the medical or dental record (dental information is considered health information and, if individually identifiable, is PHI).
2) There is no distinction between how PHI is used - e.g. health insurance claim versus dental insurance claim.
3) A dentist is clearly considered a provider under HIPAA
4) If the dentist conducts electronic transactions, then they are a covered entity and must comply with all of the HIPAA rules, including Privacy and Security.
I hope this helps,
Tom Hanks
Practice Director, Enterprise Security & HIPAA Compliance
Beacon Partners, Inc.
Hoffman Estates, IL 60195
PH: 847.490.5306
Email: tom.hanks@beaconpartners.com

********** [hipaalive] RE: GENERAL: Audit Trail Storage Requirements **********
>>> bquirey@crewshancock.com 02/02/01 02:13PM >>>
The privacy regulations (specifically the section to be codified at 45 C.F.R. § 164.528(a)(3)-found at 65 Fed. Reg. 82826) give patients the right to request an accounting of disclosures of protected health information for purposes other than treatment, payment or health care operations-for a period of up to six years prior to the date of the request.

********** [hipaalive] RE: [hipaalive]More AHA - cost savings **********

>>> MJackson@OutlookAssoc.com 02/02/01 01:14PM >>>

What about the savings to offset some of the cost?

It seems to me that AHA members could offset at least a portion of this cost by automating payment entry thru the implementation of a standard 835 ERA which will be available (in theory) for 100% of the payments coming into them once HIPAA's transactions are implemented. Manual payment entry is labor intensive and error prone. A large provider likely has many FTE's dedicated to this task. This transaction alone has the potential to bring a very large ROI (easily in the six figures for even a medium sized facility) in the first year. I would be interested in knowing if the AHA has surveyed its members to find out how many currently use this transaction and if so, what percentage of their payments are posted automatically and what cost benefits they experienced after implementation.

From one of my previous postings...

I recently read an article published by HFMA in January of 1999 written by John McBride and James Moynihan titled "EDI and Imaging Automate the Business Office". It talked about the savings experienced by Memorial Sloan-Kettering Cancer Center in New York when they implemented ERA and imaging. They were able to eliminate 22 FTE's and save $365,000 in their first year. I spoke with their Director of Patient Accounting. She stated they take in ERA's from Medicare, Medicaid and BCBS which automates approximately 50% of their payments. The ERA is then converted to a COLD image and stored for viewing, printing and faxing (this is important for secondary billing, research and patient communication). With about 400 million in revenues last year, she has 4 people performing payment entry. I've seen similar results when taking paper EOBs , scanning them and converting them to ERA.

When stored in and accessed from a database, computerized claim status can allow you to track your claim electronically and is as close as you get to sending your claim by certified mail. With an average of 15 minutes per phone call for a claim status check, I'm certain this transaction saves on labor (and long distance) but when you add to that proof of timely filing - how much did AHA members write off for that last year? Given the size of the average AHA member claim, preventing even a few siginificant losses could cover the cost of NDC code implementation.

Provider-to-Payer COB (837) is another transaction that has the potential for a significant ROI. No more matching paper EOBs to paper claims! How many secondary claims are AHA members processing by hand today?

How many FTEs are dedicated to checking eligibility and obtaining authorization?

When handled properly, HIPAA transactions can have a tremendous impact on workflow and productivity - automatically routing denied authorizations, eligibility issues, denied claims, payment exceptions, etc. to the proper individuals for follow-up. In most cases, this happens manually today.

Under HIPAA, healthcare providers finally gain control of electronic transactions. They alone have the option of implementing transaction standards and when they ask for a transaction electronically - their healthplans must comply. For perhaps the first time all providers are able to achieve the critical mass of electronic transactions necessary to see a real cost savings - even the solo practitioner. I understand the concern AHA members have in complying with HIPAA but I wonder if as much research has been done to identify the cost savings of HIPAA transactions as appears to have gone into identifying the cost. If so, I think it would be excellent contribution if AHA would share what they believe is the "net net" of HIPAA and the model they used to determine that.

Marcallee Jackson
Managing Consultant

Outlook Associates, Inc.
Long Beach, CA
(562) 432-5253

Improving Data Improving Healthcare

********** [hipaalive] RE: GENERAL: Audit Trail Storage Requirement *******
>>> tom.hanks@beaconpartners.com 02/03/01 10:13AM >>>

The audit trail function and disclosures are different animals - here are excerpts from pages 82739 & 82740 that provide guidance.

1) You can see from this excerpt that HHS understands that accounting for all disclosures is considered too burdensome. An additional conclusion may be drawn that if the disclosure is too burdensome, then an audit trail for use or viewing would also be too burdensome.

"Response: We do not accept the comments suggesting removing the exception for disclosures for treatment, payment, and health care operations. While including all disclosures within the accounting would provide more information to individuals about to whom their information has been disclosed, we believe that documenting all disclosures made for treatment, payment, and health care operations purposes would be unduly burdensome on entities and would result in accountings so voluminous as to be of questionable value. Individuals who seek treatment and payment expect that their information will be used and disclosed for these purposes. In many cases, under this final rule, the individual will have consented to these uses and disclosures. Thus, the additional information that would be gained from including these disclosures would not outweigh the added burdens on covered entities. We believe that retaining the exclusion of disclosures to carry out treatment, payment, and health care operations makes for a manageable accounting both from the point of view of entities and of individuals. We have conformed the language in this section with language in other sections of the rule regarding uses and disclosures to carry out treatment, payment, and health care operations. See § 164.508 and the corresponding preamble discussion regarding our decision to use this language."

2) While the following quote defines the difference between accounting and disclosure. Audit trails are clearly anticipated to be record of alternation of records, not record when used or viewed. Even if the audit trail recorded when information was used or viewed it would not contain the information required for disclosure accounting.

"Response: Audit trails and the accounting of disclosures serve different functions. In the security field, an audit trail is typically a record of each time a sensitive record is altered, how it was altered and by whom, but does not usually record each time a record is used or viewed. The accounting required by this rule provides individuals with information about to whom a disclosure is made. An accounting, as described in this rule, would not capture uses. To the extent that an audit trail would capture uses, consumers reviewing an audit trail may not be able to distinguish between accesses of the protected health information for use and accesses for disclosure. Further, it is not clear the degree to which the field is technologically poised to provide audit trails. Some entities could provide audit trails to individuals upon their request, but we are concerned that many could not. We agree that it is important to coordinate this provision of the privacy rule with the Security Rule when it is issued as a final rule."

Tom Hanks
Practice Director, Enterprise Security & HIPAA Compliance
Beacon Partners, Inc.
Hoffman Estates, IL 60195
PH: 847.490.5306
Email: tom.hanks@beaconpartners.com